

Estimating the eigenstates of an unknown density operator without damaging it

Jingliang Gao · Feng Cai

Received: date / Accepted: date

Abstract Given n qubits prepared according to the same unknown density operator ρ , we propose a nondestructive measuring method which approximately yields the eigenstates of ρ . It is shown that, for any plane which passes through the center point of the Bloch sphere, there exists corresponding projective measurement. By performing these measurements, we can scan the whole Bloch sphere like radar to search for the orientation of ρ and determine the eigenstates. We show the convergency of the measurements in the limit $n \rightarrow \infty$. This result actually reveals a mathematical structure of the n -fold Hilbert space .

Keywords quantum estimation · eigenstate · typical subspace

PACS 03.67.-a · 03.65.Wj

1 Introduction

The quantum state estimation(or say quantum tomograph)[1,2,3,4,5,6] is the task of inferring the density operator ρ of a quantum system by appropriate measurements. Like a classical probability distribution it cannot be measured on a single system, but can only be estimated on an ensemble sequence of identically prepared systems. Since ρ can be spectral decomposed as $\rho = \sum_i p_i |e_i\rangle\langle e_i|$, the estimation of ρ can be divided into two parts: the estimation of the spectrum $\{p_i\}$ and the estimation of the eigenstates $\{|e_i\rangle\}$. If we do not mind damaging the state, we can take measurements on each copy

Jingliang Gao
State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071,
China
E-mail: gaojl0518@gmail.com

Feng Cai
xidian University

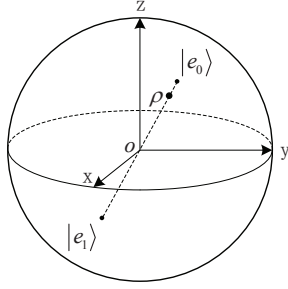


Fig. 1: Bloch sphere

of ρ and the estimations are simple. However, if we want the estimations are nondestructive, then the question becomes challenging. Instead of measuring each state individually, we need collective operations on all n states simultaneously. For the spectrum, Keyl and Werner[1] proposed a scheme based on the irreducible representations of permutation group and showed that the Young frame is a good estimation. On the other hand, it is still unclear that what kind of mathematical structure can be used to estimate the eigenstates. In this paper, we focus on this problem and try to give a solution for the qubit systems.

It is well known that a qubit system can be geometrically represented as a Bloch sphere[7]. Suppose the spectrum decomposition of ρ is $\rho = p|e_0\rangle\langle e_0| + (1-p)|e_1\rangle\langle e_1|$, then the eigenstates $|e_0\rangle, |e_1\rangle$ are determined by the axis $o\rho$ (see Fig.1). To estimate $|e_0\rangle$ and $|e_1\rangle$, we only need to know the orientation of the axis $o\rho$. Furthermore, the axis $o\rho$ is determined by the plane $z o\rho$ and the plane $y o\rho$, so the estimation of $|e_0\rangle, |e_1\rangle$ reduces to estimate the orientation of the plane $z o\rho$ and $y o\rho$. In the following, we will show that, for any plane which passes through the center point of the Bloch sphere, there exists a corresponding subspace in the n -fold Hilbert space. The projective measurement onto the subspace can distinguish whether ρ lies in the plane or not. Successively performing these measurements, we can scan the Bloch sphere to locate the plane $z o\rho$ and $y o\rho$. It will be shown that this measuring scheme scarcely disturb the state if n is sufficiently large.

2 Estimation of the eigenstates

Before giving the main results, we briefly introduce the strongly typical set[9] which will be very useful for understanding our estimating method. We use the notation x^n to denote a classical binary sequence x_0, x_1, \dots, x_n . k is the number of 0 in x^n . For a binary distribution $Q = (q, 1-q)$, the strongly typical set $A_\varepsilon^n(q)$ is defined as:

$$A_\varepsilon^n(q) = \left\{ x^n : \left| \frac{k}{n} - q \right| \leq \frac{\varepsilon}{2} \right\} \quad (1)$$

When ε is small, $A_\varepsilon^n(q)$ is the collection of the sequences for which the number of 0 is about nq , and the number of 1 is about $n(1-q)$.

Now we explain how to estimate the plane zop . Define a basis $\{|e_0^\varphi\rangle, |e_1^\varphi\rangle\}$ by:

$$|e_0^\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle), |e_1^\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\varphi}|1\rangle)$$

Clearly, this basis is corresponding to a diameter of the circle xoy . Let $\rho^\varphi = \langle e_0^\varphi | \rho | e_0^\varphi \rangle |e_0^\varphi\rangle\langle e_0^\varphi| + \langle e_1^\varphi | \rho | e_1^\varphi \rangle |e_1^\varphi\rangle\langle e_1^\varphi|$, then ρ^φ corresponds to the projection of ρ onto the basis $\{|e_0^\varphi\rangle, |e_1^\varphi\rangle\}$ (see Fig.2).

Construct a “yes/no” measurement $\{M_{yes}^\varphi, M_{no}^\varphi\}$ by

$$M_{yes}^\varphi = \sum_{x^n \in A_\varepsilon^n(\frac{1}{2})} |e_{x_1}^\varphi\rangle\langle e_{x_1}^\varphi| \otimes |e_{x_2}^\varphi\rangle\langle e_{x_2}^\varphi| \otimes \dots |e_{x_n}^\varphi\rangle\langle e_{x_n}^\varphi|$$

$$M_{no}^\varphi = I - M_{yes}^\varphi$$

Perform this measurement on $\rho^{\otimes n}$, then we get the result “Yes” with probability $\text{tr}(M_{yes}^\varphi \rho^{\otimes n})$.

Proposition1 For any $\varepsilon > 0$ and $\delta > 0$, when n is sufficiently large, we have

(1-a) If $\|\rho^\varphi - I/2\| \leq \varepsilon$, then

$$\text{tr}(M_{yes}^\varphi \rho^{\otimes n}) \geq 1 - \delta \quad (2)$$

where $\|\cdot\|$ is trace norm.

(1-b) If $\|\rho^\varphi - I/2\| > \varepsilon$, then

$$\text{tr}(M_{yes}^\varphi \rho^{\otimes n}) \leq \delta \quad (3)$$

(1-c) Let F^φ be the entanglement fidelity[7] of the measurement, then

$$F^\varphi \geq 1 - 2\delta \quad (4)$$

$I/2$ is the center o of the Bloch sphere. Because ρ^φ is the projection of ρ onto the basis $\{|e_0^\varphi\rangle, |e_1^\varphi\rangle\}$, the condition $\|\rho^\varphi - I/2\| \leq \varepsilon$ implies that ρ lies in a thin layer which takes o as center and is perpendicular to the basis $\{|e_0^\varphi\rangle, |e_1^\varphi\rangle\}$ and is ε thick(see Fig.2(a)). The proposition(1-a) reveals that if ρ lies in the layer, the measurement will almost always give the result “Yes”. Proposition(1-b) reveals that if ρ is outside the layer(see Fig.2(b)), the result will almost always be “No”. So the measurement can distinguish whether ρ lies in the thin layer or not. Since the parameter ε can be as small as desired, the layer can be viewed as a plane. If the layer contains ρ , the layer approximate to the plane zop ! Furthermore, because δ can be arbitrary small, the measurement

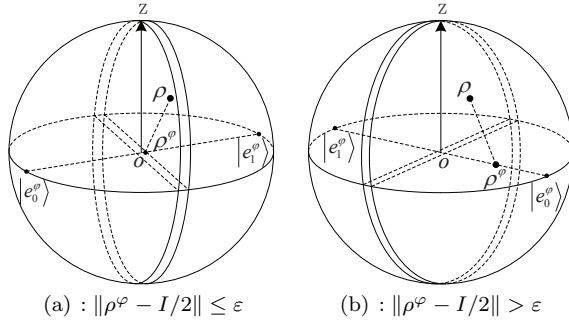


Fig. 2: Geometric interpretation of Proposition1

fidelity F^φ is arbitrarily close to 1, which means that the measurement scarcely disturb $\rho^{\otimes n}$. Consequently, we can construct a sequence of measurements to find the plane $zορ$. We begin with the measurement $\{M_{yes}^{\varphi=0}, M_{no}^{\varphi=0}\}$, if we get the result “Yes”, then $zορ$ is found; If “No”, perform the next measurement $\{M_{yes}^{\varphi=\varepsilon}, M_{no}^{\varphi=\varepsilon}\}$. If we get the result “Yes”, then the work is done; If “No”, perform the next measurement $\{M_{yes}^{\varphi=2\varepsilon}, M_{no}^{\varphi=2\varepsilon}\}$; As φ increases, the layer rotates about the z -axis and scans the whole Bloch sphere gradually. Repeat the above procedures until for some φ we get a “Yes”, then the orientation of $zορ$ is got.

A problem of this estimation scheme is that the fidelity decreases with the increasing times of measurement. However, this problem can be overcome if n is large enough. Proposition(1-c) tell us that for any ε and δ , there exist a positive number $N(\varepsilon, \delta)$, if $n > N(\varepsilon, \delta)$, then $F^\varphi > 1 - \delta$. Suppose we need m times of measurement to find $zορ$ and the whole fidelity is F . Then we can reasonably assume that $F > 1 - f(m, \delta)$, where $f(m, \delta)$ is a continuous increasing function on δ and m and $f(m, 0) = 0$, $f(1, \delta) = \delta$. For a given ε , m is up to $\frac{\pi}{\varepsilon}$ because the measurement interval is ε . We can choose δ^* such that $f(\frac{\pi}{\varepsilon}, \delta^*) \approx 0$, and choose n such that $n > N(\varepsilon, \delta^*)$. In this case, $F > 1 - f(m, \delta^*) > 1 - f(\frac{\pi}{\varepsilon}, \delta^*)$, so $F \approx 1$. In other word, when n is large enough, F will be close to 1.

The plane $yορ$ can be estimated in the same way. We can define a basis $\{|e_0^\theta\rangle, |e_1^\theta\rangle\}$ as

$$|e_0^\theta\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} |1\rangle, \quad |e_1^\theta\rangle = \sin \frac{\theta}{2} |0\rangle - \cos \frac{\theta}{2} |1\rangle$$

This basis corresponds to a diameter of the circle $xοz$.

Construct a measurement $\{M_{yes}^\theta, M_{no}^\theta\}$ by

$$M_{yes}^\theta = \sum_{x^n \in A_\varepsilon^n(\frac{1}{2})} |e_{x_1}^\theta\rangle\langle e_{x_1}^\theta| \otimes |e_{x_2}^\theta\rangle\langle e_{x_2}^\theta| \otimes \dots |e_{x_n}^\theta\rangle\langle e_{x_n}^\theta|$$

$$M_{no}^\theta = I - M_{yes}^\theta$$

Similarly, this measurement can tell us whether or not ρ lies in the thin layer which is perpendicular to the basis $\{|e_0^\theta\rangle, |e_1^\theta\rangle\}$, and such a measurement scarcely disturb $\rho^{\otimes n}$. As θ increases, the layer rotates about the y -axis. Thus a measuring sequence can be constructed to find $y\rho$.

3 Proof of the Proposition

Proving Proposition 1 is quite a mathematical work and we need some knowledge about the method of types [8, 9] which was developed by Csiszar and Korner. We still use x^n to denote a binary sequence x_0, x_1, \dots, x_n and k is the number of 0 in x^n .

The type P_x of x^n is the relative proportion of 0 and 1, i.e. $P_x(0) = k/n$, $P_x(1) = 1 - k/n$. The collection of sequences of type P is called the type class of P , denoted as $T(P)$, i.e. $T(P) = \{x^n : P_x = P\}$. $|T(P)|$ is the number of elements in $T(P)$, then

$$|T(P)| \leq 2^{nH(P)} \quad (5)$$

where $H(\cdot)$ is the Shannon entropy function.

The strongly typical set $A_\varepsilon^n(q)$ can be stated as

$$A_\varepsilon^n(q) = \bigcup_{P: |P(0) - q| \leq \frac{\varepsilon}{2}} T(P) \quad (6)$$

If we produce binary sequence according to the distribution $Q = (Q_0, Q_1)$, $Q_0 = q$, then $A_\varepsilon^n(q)$ is a high probability set, i.e. for any fixed $\varepsilon > 0$ and $\delta > 0$, when n is large enough,

$$Pr\{x^n \in A_\varepsilon^n(q)\} = \sum_{x^n \in A_\varepsilon^n(q)} Q(x^n) \geq 1 - \delta \quad (7)$$

where $Q(x^n) = Q_{x_1} Q_{x_2} \cdots Q_{x_n}$ is the probability that x^n occurs. This property reveals that if we produce binary sequences according to the distribution Q , then the sequences are practically always in $A_\varepsilon^n(q)$. Furthermore, we give a stronger lemma.

Lemma 1: *Given q , for any distribution $Q' = (q', 1 - q')$ which satisfies $|q' - q| \leq \frac{\varepsilon}{2}$, $A_\varepsilon^n(q)$ is a high probability set, i.e. for any fixed $\varepsilon > 0$ and $\delta > 0$, when n is large enough,*

$$\sum_{x^n \in A_\varepsilon^n(q)} Q'(x^n) \geq 1 - \delta \quad (8)$$

where $Q'(x^n) = Q'_{x_1} Q'_{x_2} \cdots Q'_{x_n}$.

This lemma tell us that if Q' is very close to Q , then $A_\varepsilon^n(q)$ is also a high probability set of Q' .

Proof: It is easy to show that $A_\varepsilon^n(q)$ contains a subset $A_{\varepsilon'}^n(q')$. Let $\varepsilon' = \varepsilon - 2|q' - q|$. Given $|q' - q| \leq \frac{\varepsilon}{2}$, it can be verified that if $|\frac{k}{n} - q'| \leq \frac{\varepsilon'}{2}$, then $|\frac{k}{n} - q| \leq \frac{\varepsilon}{2}$. So $A_{\varepsilon'}^n(q') \subseteq A_\varepsilon^n(q)$. Thus we have

$$\sum_{x^n \in A_\varepsilon^n(q)} Q'(x^n) \geq \sum_{x^n \in A_{\varepsilon'}^n(q')} Q'(x^n) \geq 1 - \delta \quad (9)$$

The second inequality follows from (7).

Now we can prove the proposition1.

Proof: Let $Q_0^\varphi = \langle e_0^\varphi | \rho | e_0^\varphi \rangle$, $Q_1^\varphi = \langle e_1^\varphi | \rho | e_1^\varphi \rangle$, then $\rho^\varphi = Q_0^\varphi |e_0^\varphi\rangle\langle e_0^\varphi| + Q_1^\varphi |e_1^\varphi\rangle\langle e_1^\varphi|$. Since $I/2$ can be decomposed as $I/2 = \frac{1}{2}|e_0^\varphi\rangle\langle e_0^\varphi| + \frac{1}{2}|e_1^\varphi\rangle\langle e_1^\varphi|$, we have

$$\begin{aligned} \|\rho^\varphi - I/2\| &= \text{tr} \left| \left(Q_0^\varphi - \frac{1}{2} \right) |e_0^\varphi\rangle\langle e_0^\varphi| + \left(Q_1^\varphi - \frac{1}{2} \right) |e_1^\varphi\rangle\langle e_1^\varphi| \right| \\ &= |Q_0^\varphi - \frac{1}{2}| + |Q_1^\varphi - \frac{1}{2}| \\ &= |Q_0^\varphi - \frac{1}{2}| + |1 - Q_0^\varphi - \frac{1}{2}| \\ &= 2|Q_0^\varphi - \frac{1}{2}| \end{aligned}$$

First we prove (1-a). The condition $\|\rho^\varphi - I/2\| \leq \varepsilon$ is equivalent to $|Q_0^\varphi - \frac{1}{2}| \leq \frac{\varepsilon}{2}$. From Lemma1, we know that for the distribution $Q^\varphi = (Q_0^\varphi, Q_1^\varphi)$,

$$\sum_{x^n \in A_\varepsilon^n(\frac{1}{2})} Q^\varphi(x^n) \geq 1 - \delta \quad (10)$$

where $Q^\varphi(x^n) = Q_{x_1}^\varphi Q_{x_2}^\varphi \dots Q_{x_n}^\varphi$.

$$\begin{aligned} \text{tr}(M_{yes}^\varphi \rho^{\otimes n}) &= \sum_{x^n \in A_\varepsilon^n(\frac{1}{2})} \langle e_{x_1}^\varphi e_{x_2}^\varphi \dots e_{x_n}^\varphi | \rho^{\otimes n} | e_{x_1}^\varphi e_{x_2}^\varphi \dots e_{x_n}^\varphi \rangle \\ &= \sum_{x^n \in A_\varepsilon^n(\frac{1}{2})} \prod_{i=1}^n \langle e_{x_i}^\varphi | \rho | e_{x_i}^\varphi \rangle \\ &= \sum_{x^n \in A_\varepsilon^n(\frac{1}{2})} Q_{x_1}^\varphi Q_{x_2}^\varphi \dots Q_{x_n}^\varphi \\ &= \sum_{x^n \in A_\varepsilon^n(\frac{1}{2})} Q^\varphi(x^n) \geq 1 - \delta \end{aligned}$$

So Proposition(1-a) is proven.

Next we give the proof of (1-b). For any type class $T(P)$ with $P = (P_0, P_1)$, we have

$$\begin{aligned}
& \sum_{x^n \in T(P)} \langle e_{x_1}^\varphi e_{x_2}^\varphi \dots e_{x_n}^\varphi | \rho^{\otimes n} | e_{x_1}^\varphi e_{x_2}^\varphi \dots e_{x_n}^\varphi \rangle \\
&= \sum_{x^n \in T(P)} \prod_{i=1}^n \langle e_{x_i}^\varphi | \rho | e_{x_i}^\varphi \rangle \\
&= \sum_{x^n \in T(P)} \langle e_0^\varphi | \rho | e_0^\varphi \rangle^{nP_0} \langle e_1^\varphi | \rho | e_1^\varphi \rangle^{nP_1} \\
&= \sum_{x^n \in T(P)} 2^{n[P_0 \log Q_0^\varphi + P_1 \log Q_1^\varphi]} \\
&= \sum_{x^n \in T(P)} 2^{-n[H(P) + D(P||Q^\varphi)]} \\
&\leq 2^{nH(P)} 2^{-n[H(P) + D(P||Q^\varphi)]} \\
&= 2^{-nD(P||Q^\varphi)}
\end{aligned}$$

where $D(P||Q^\varphi)$ is the relative entropy[9] between P and Q^φ . The second equality holds because for any sequence x^n with type P , the number of 0 is nP_0 and the number of 1 is nP_1 . The inequality is due to (5). Because $A_\varepsilon^n(\frac{1}{2})$ can be decomposed as (6), we have

$$\begin{aligned}
\text{tr}(M_{yes}^\varphi \rho^{\otimes n}) &= \sum_{x^n \in A_\varepsilon^n(\frac{1}{2})} \langle e_{x_1}^\varphi e_{x_2}^\varphi \dots e_{x_n}^\varphi | \rho^{\otimes n} | e_{x_1}^\varphi e_{x_2}^\varphi \dots e_{x_n}^\varphi \rangle \\
&= \sum_{P: |P_0 - \frac{1}{2}| \leq \frac{\varepsilon}{2}} \sum_{x^n \in T(P)} \prod_{i=1}^n \langle e_{x_i}^\varphi | \rho | e_{x_i}^\varphi \rangle \\
&\leq \sum_{P: |P_0 - \frac{1}{2}| \leq \frac{\varepsilon}{2}} 2^{-nD(P||Q^\varphi)} \\
&\leq \sum_{P: |P_0 - \frac{1}{2}| \leq \frac{\varepsilon}{2}} 2^{-n \min_P D(P||Q^\varphi)} \\
&\leq (n+1) \cdot 2^{-n \min_P D(P||Q^\varphi)} \\
&= 2^{-n[\min_P D(P||Q^\varphi) - \frac{\log n+1}{n}]}
\end{aligned}$$

The third inequality holds because there are at most $n+1$ types for binary sequences of length n .

The condition $\|\rho^\varphi - I/2\| > \varepsilon$ is equivalent to $|Q_0^\varphi - \frac{1}{2}| > \frac{\varepsilon}{2}$. Combined with $|P_0 - \frac{1}{2}| \leq \frac{\varepsilon}{2}$, we get $Q_0^\varphi \neq P_0$, so $D(P||Q^\varphi) > 0$. Thus when n is large enough, $2^{-n[\min_P D(P||Q^\varphi) - \frac{\log n+1}{n}]}$ can be arbitrarily small, i.e. for any $\delta > 0$, $\text{tr}(M_{yes}^\varphi \rho^{\otimes n}) < \delta$.

The proof of (1-c) is very simple. According to[7], for any quantum operation $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$, the entanglement fidelity $F(\rho, \mathcal{E}) = \sum_k |\text{tr}(E_k \rho)|^2$.

So for the measurement $\{M_{yes}^\varphi, M_{no}^\varphi\}$,

$$\begin{aligned} F^\varphi &= |tr(M_{yes}^\varphi \rho^{\otimes n})|^2 + |tr(M_{no}^\varphi \rho^{\otimes n})|^2 \\ &\geq |1 - \delta|^2 \geq 1 - 2\delta \end{aligned}$$

This complete our proof.

4 Conclusion

In this paper, we proposed a method for estimating the eigenstates of ρ . We show that the orientation of $z\rho$ and $y\rho$ can be found via a sequence of “yes/no” measurements and then the eigenstates can be determined.

Acknowledgements This work is supported by the National Natural Science Foundation of China Grant No.61271174, No.61372076 and No.61301178.

References

1. Keyl, M., Werner, R. F.: Estimating the spectrum of a density operator, Phys. Rev. A, 64, 052311 (2001)
2. Keyl, M.: Quantum state estimation and large deviations, Reviews in Mathematical Physics, 18, 19 (2006)
3. Bagan, E., Ballester, M. A., Gill, R. D., Monras, A., Munoz-Tapia, R.: Optimal full estimation of qubit mixed states, Phys. Rev. A, 73, 032301 (2006)
4. Gross, D., Liu, Y. K., Flammia, S. T., Becker, S., Eisert, J.: Quantum state tomography via compressed sensing, Phys. Rev. Lett, 105, 150401 (2010)
5. Christandl, M., Renner, R.: Reliable Quantum State Tomography, Phys. Rev. Lett, 109, 120403 (2012)
6. Bennett, C. H., Harrow, A. W., Lloyd, S.: Universal quantum data compression via nondestructive tomography, Phys. Rev. A, 73, 032336 (2006)
7. Nielsen, M. A., Chuang, I. L.: Quantum computation and quantum information. Cambridge University Press (2000)
8. Csiszar, I., Körner, J.: Information Theory: Coding Theorems for Discrete Memoryless Systems. Cambridge University Press (2011)
9. Cover, T. M., Thomas, J. A.: Elements of Information Theory. John Wiley & Sons (2012)

